Flight Critical Data Integrity Assurance for COTS based Ground Components

Yann-Hang Lee
Computer Science & Engineering Department
Arizona State University
Tempe, AZ 85287

Jim Krodel
Pratt & Whitney
East Hartford, CT 06108

Agenda

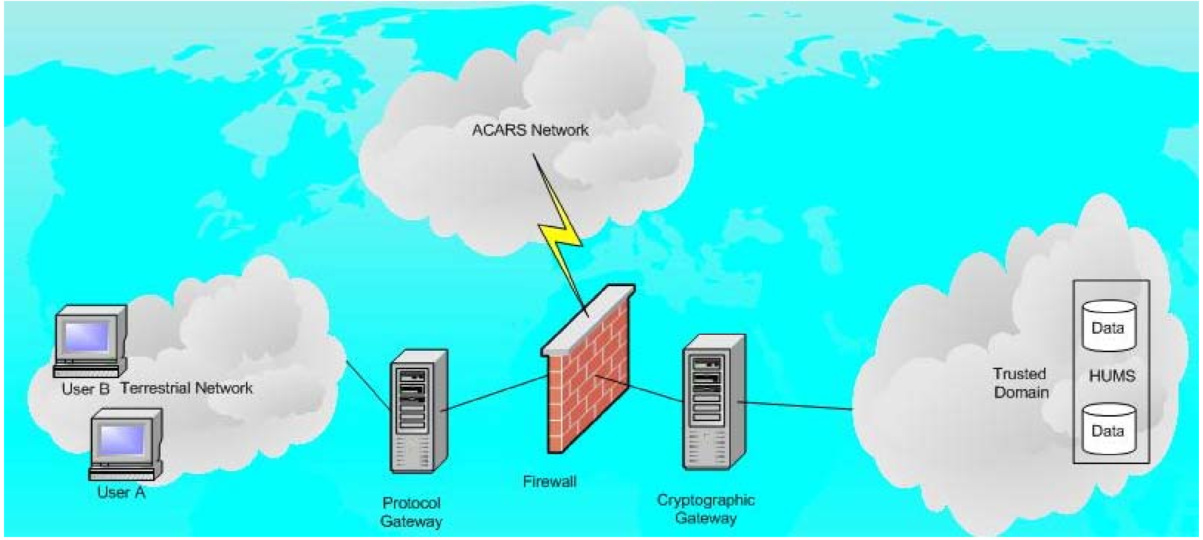
- **HUMS Architecture**
- **Existing Guidelines and Related Work**
  - Rotorcraft HUMS Advisory Circular (AC-27-1 / AC-29-2)
- **Analysis for HUMS**
  - Hazard Analysis for System Safety
  - Vulnerability Analysis for Security
- **A Case Study -- Applicability of DO278 to HUMS**
- **Summary**

Research Supported by SDSS

- **Ground processing systems are likely to use commercial-off-the-shelf (COTS) software and hardware for maintaining flight critical data.**
  - CNS/ATM (Communication, Navigation, Surveillance/Air Traffic Management) and HUMS (Health/Usage Monitoring System)
- **In Rotorcraft HUMS,**
  - flight data and maintenance records can be easily collected, analyzed, and disseminated
  - helicopter parts are assigned a safe-life limits based on the aircraft’s usage and maneuvers
- **Investigate the issues in making a COTS ground processing system for aircraft maintenance trustworthy and secure.**
  - Process and objectives for data integrity in COTS ground systems
  - Information and data protection, access security

HUMS – Architecture Assumption

- **On-board HUMS and ACARS, HUMS database servers, and clients**
- **Three major components:**
  - Data communication: between On-board HUMS, HUMS data server and clients
  - Data processing for raw and formatted data to compute "Calculated Retirement Time" for helicopter parts
  - Data storage: data base and mass storage devices



Existing Guidelines

- **DO-178B**
  - acts as a guideline for determining that an acceptable level of confidence is present in the software aspects of airborne systems
  - both process and product assurance based assurance
- **DO-278**
  - based on DO-178B for CNS/ATM
  - a section devoted mainly to software development with COTS software components in four processes (planning, acquisition, verification, and configuration management).
- **Rotorcraft HUMS Advisory Circular (AC-27-1 / AC-29-2) for certifying HUMS ground based systems that contain COTS components**

HUMS AC

- **Developed by the Rotorcraft Health Use Monitoring System Advisory Guidance (RHUMSAG)**
- **Determine the end-to-end criticality by performing a Functional Hazard Analysis (FHA) including the ground component**
- **Unique development of a HUMS system**
  - the application software, perhaps level A under DO-178B could be integrated with COTS software that may be at level D
- **Provide guidance to achieve airworthiness approval for three basic aspects of HUMS certification**
  - Rotorcraft HUMS installation: all equipment needed for the end-to-end application
  - Credit validation
  - Instructions for Continued Airworthiness (ICA): assurance for the parts that could change with time or use.

HUMS AC

- **COTS in HUMS AC:**
  - defined as equipment, hardware and software, that is not qualified to aircraft standards
  - in DO178, “Commercial off-the-shelf (COTS) software” – Commercially available applications sold by vendors through public catalog listings
- **Mitigating Action: an autonomous and continuing compensating factor or process that may**
  - modify the level of qualification associated with certification of a HUMS application.
- **Independent Verification Means: To gain confidence, an independent process is used to verify the correct functionality of a HUMS application on a ground station that utilizes COTS.**

Motivation of HUMS AC

- **To reduce the cost of the system by allowing the use of COTS components**
- **Still need to ensure flight safety.**
  - Example errors that can jeopardize flight safety if they appear in aviation software.
    - Halts during execution, overflows, variations in time response, hardware and software incompatibilities, hardware failures, unbounded recursive algorithms, bad stack usage, resource contention, task conflicts, bad interaction with other systems, etc.,
  - However, these types of errors may not have any influence on the flight safety if they occurred in HUMS.
- **In HUMS, data integrity must be ensured.**
  - COTS not directly related to the manifestation of vehicle part action (i.e. correctness and accuracy for the predicted vehicle part action)
  - COTS directly related to such action.

HUMS and COTS

- **HUMS characteristics**
  - non-time-critical
  - possible human intervention
- **Mitigating action and independent verification means are targeted to data integrity**
  - no corrupted data in computation and decision
  - information is protected
- **However, when trying to apply an effective service history**
  - problematic data collection practices,
  - problematic interpretations
  - the associated assumptions are moving targets.
  - the AC statement of “satisfactory service history” may just mean the HUMS applications or COTS components !!

Related Work

- HUMS in military aircrafts
  - improve readiness, streamlined maintenance practices
- Bell BA-609 and Sikorsky S-76/S-92 HUMS for credit projects
- FAA R&D project with NRTC/RITA to demonstrate open architecture
- FAA R&D project with Navy to define minimum acceptable system capabilities

Related Work (Cont'd)

- **A case study of COTS in certified nuclear tester for ICBM**
  - use COTS to replace the outdated tester (built in 1960) to reduce design cycle time and costs.
  - The absolute necessity of a planning, requirement, design approval and certification process
  - Sometimes COTS capabilities may have to be augmented by the use of a wrapper (fence) to incorporate safety and security guarantees.
- **DO-200A Database Integrity**
  - data for navigation and flight management must be subjected to certification requirement and the quality (i.e. accuracy, resolution, and integrity) must be assured.
  - "*data quality*" criteria and *"aeronautical data chain"*
  - emphasize in data transmission and preparation (processing)

Hazard Analysis for System Safety

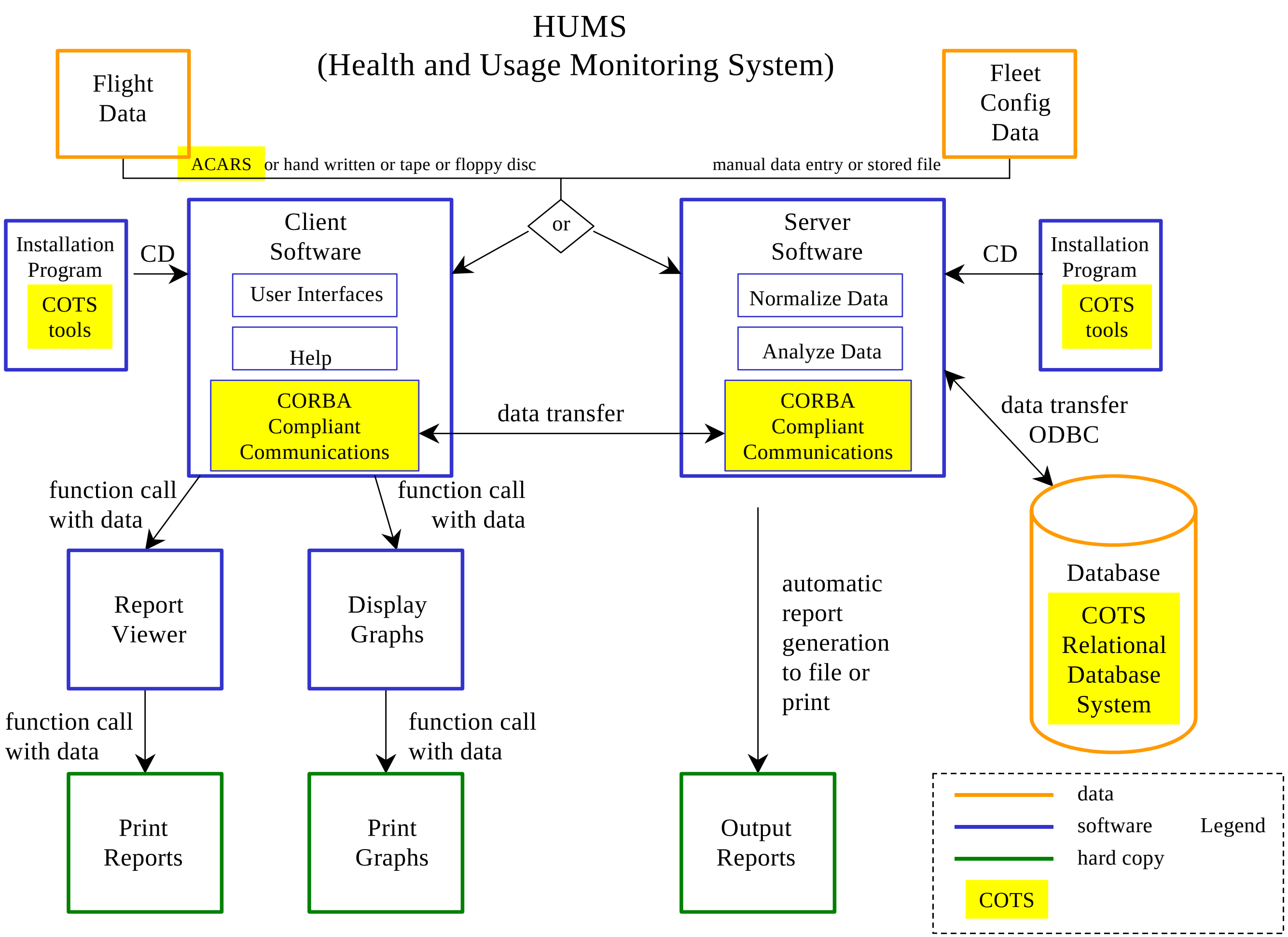
	HUMS Subsystem under consideration	Hazard (Critical Event)	Causal Analysis		Mitigation Technique
1	ACARS	Data can be corrupted during transmission.	Noise on communication channel.	Important data can be corrupted.	Message digests should be used to ensure data integrity.
10	HUMS DB	The DB goes down and when brought up again, it is in an inconsistent state.	Efficient check pointing mechanism not employed.	The data is in an inconsistent state.	Checkpointing mechanism should be employed. Redundancy should be used for alternate forms.
21	HUMS INTERFACE TO CLIENT APPLICATION	Client software does not support SSL/Encryption.	Outdated software being used by client.	Client will not be able to connect to the HUMS.	Specifications for the client machine and software should be provided.

Vulnerability Analysis for Security

	HUMS Subsystem under consideration	Threat	Effect	Mitigation Technique
1	ACARS	Data can be intercepted during transmission by hackers.	Unauthorized access gained to important data.	Encryption should be used during transmission.
6	HUMS DB	Attacker compromises the secret key used for validating ACARS.	An attacker can now pretend to be the ACARS node that is sending data to the HUMS.	Efficient key management must be employed. Also, key lengths should be longer, and key setup techniques should be chosen properly.
9	COTS SOFTWARE	Attackers can exploit bugs and other vulnerabilities in software.	Trojans, backdoors, bugs, and other vulnerabilities can result in compromise of sensitive information.	Bug reports and mailing lists of COTS components should be periodically checked to ensure that all patches are duly installed.

A Case Study with a Commercial Database

- Use the COTS-specific guidance of DO-278



Process and Objectives for Handling Flight Information

- **Looked into the objectives of the DO278 and their applicability within a COTS context.**
- **The example COTS database maintains an extensive web site that contains a great deal of information about their products. The vendor also encourages communication within their user community.**
- **Example observation:**
  - Objective: Item b. in section 4.1.5.1 of DO-278 "The adequacy of life cycle data available for assurance purposes is determined." [23]
  - The life cycle data for this database was not readily available, and no evaluation as to the adequacy of the COTS life cycle data has been made
  - Lack of support for older versions. If the COTS components are upgraded to be current version, then the vendors will more likely support the COTS components.

Applicability of DO278 to MS Windows

- Used Microsoft Access (COTS related to vehicle part action) an analyzed the applicability of the DO278 objectives, giving a rationale as to why/why not. e.g.

Annex A Ref.	Objective	Para. Ref.	AL1	AL2	AL3	AL4	AL5	HUMS Demo System MS Access
1-1	Software development and integral processes activities are defined. (A-1,1)	4.1a 4.3	R	R	R	R	R	**Partial**: Some of the listed activities for this objective are: Setting dev standards, Tools for error prevention, use of change control, error avoidance and so on. Since the software is purchased off the shelf, seldom are we provided with these details as they are proprietary. e.g on the Microsoft website absolutely no information is provided as to the process followed, tools used and so on. Only installation and end user information is given. CMM Level 2 could meet this objective / Need to consider installation as an integral process / The configuration of the windows OS should be defined
1-2	Transition criteria, inter-relationships and sequencing among processes are defined.	4.1b 4.3	R	R	R	R		**N/A**: The software life cycle process followed is not always well documented. Also different parts of the product follow different life cycles not available to us. MS company is a team developed product which many times is rapid prototyped. Hence defined process and sequence order does not exist.

Applicability of DO278 to MS Access

- Used Microsoft Windows OS (COTS not related to vehicle part action) an analyzed the applicability of the DO278 objectives, giving a rationale as to why/why not. e.g.

Annex A Ref.	Objective	Para. Ref.	AL1	AL2	AL3	AL4	AL5	HUMS Demo System OS
1-1	Software development and integral processes activities are defined. (A-1,1)	4.1a 4.3	R	R	R	R	R	**Partial**: Some of the listed activities for this objective are: Setting dev standards, Tools for error prevention, use of change control, error avoidance and so on. Since the software is purchased off the shelf, seldom are we provided with these details as they are proprietary. e.g on the Microsoft website absolutely no information is provided as to the process followed, tools used and so on. Only installation and end user information is given. CMM Level 2 could meet this objective / Need to consider installation as an integral process / The configuration of the windows OS should be defined
1-2	Transition criteria, inter-relationships and sequencing among processes are defined.	4.1b 4.3	R	R	R	R		**N/A**: The software life cycle process followed is not always well documented. Also different parts of the product follow different life cycles not available to us. MS company is a team developed product which many times is rapid prototyped. Hence defined process and sequence order does not exist.

Observations

- **COTS has little information on development process**
- **COTS is changing (versions and service packs) and has various configurations**
  - a running target in planning, requirement, design approval, and certification steps
- **For HUMS applications, data integrity is the main concern**
- **Assessment of alternate approaches for acceptance of COTS software**
  - Alternate approval process
  - Alternate product assurance approaches
  - Example: use wrapper and redundancy to augment COTS capability in a nuclear certifiable tester for the Minuteman III ICBM

Organization of Final Report

- **Section 1 – Introduction**
- **Section 2 –**
  - The use of COTS components, their advantages, and the challenges that they pose towards the building of a safe and secure system.
- **Section 3 –**
  - HUMS is defined and the various issues of safety and security that deserve attention are highlighted.
- **Section 4 –**
  - the current guidance that is available relating to COTS and ground-based systems.
  - the guidelines available in the DO-278 pertaining to helping plan, acquire, verify, and manage the use of COTS software.
  - HUMS AC and COTS approaches in the AC

Organization of Final Report (Cont'd)

- **Section 5 –**
  - the current and emerging industry approaches with regard to safety and security
  - the vulnerabilities that airborne data is prone to and ways in which it can be protected
  - hazard analysis, threat analysis, and mitigations
- **Section 6 –**
  - data integrity of COTS-based ground systems
  - the HUMS is used as a representative ground-based system to see how the objectives of the DO-278 can be applied (to MS Windows and MS Access) at AL4.
  - The other case study in a HUMS system with a commercial database system
- **Section 7 – summary**

Summary

- **Investigated the issues surrounding the use of COTS components to ensure data integrity of flight critical data in HUMS systems**
  - safety and security
  - the existing guidance for the use of COTS components
  - the objectives of current guidance from the point of view of applicability and shortcomings
  - hazard analysis and vulnerability analysis as a means for developing an effective risk mitigation strategy
- **Case studies and demonstration project**